PART 11—SECURITY CLASSIFICATION REGULATIONS PURSUANT TO EXECUTIVE ORDER 11652

Sec.

AUTHORITY: Executive Order 11652 (37 FR 5209, March 10, 1972) and the National Security Directive of May 17, 1972 (37 FR 10053, May 19, 1972).

SOURCE: 37 FR 23541, Nov. 4, 1972, unless otherwise noted.

§ 11.1 Purpose.

These regulations establish policy and procedures governing the classification and declassification of national security information. They apply also to information or material designated under the Atomic Energy Act of 1954, as amended, as ''Restricted Data,'' or ''Formerly Restricted Data'' which, additionally, is subject to the provisions of the Act and regulations of the Atomic Energy Commission.

§ 11.2 Background.

While the Environmental Protection Agency does not have the authority to originally classify information or material in the interest of the national security, it may under certain circumstances downgrade or declassify previously classified material or generate documents incorporating classified information properly originated by other agencies of the Federal Government which must be safeguarded. Agency policy and procedures must conform to applicable provisions of Executive Order 11652, and the National Security Council Directive of May 17, 1972, governing the safeguarding of national security information.

§ 11.3 Responsibilities.

(a) Classification and Declassification Committee: This committee, appointed by the Administrator, has the authority to act on all suggestions and complaints with respect to EPA's administration of this order. It shall establish procedures to review and act within 30 days upon all applications and appeals regarding requests for declassification. The Administrator, acting through the committee, shall be authorized to overrule previous determinations in whole or in part when, in its judgment, continued protection is no longer required. If the committee determines that continued classification is required under section 5(B) of Executive Order 11652, it shall promptly so notify the requester and advise him that he may appeal the denial to the Interagency Classification Review Committee.

(b) Director, Security and Inspection Division, Office of Administration: The Director, Security and Inspection Division, is responsible for the overall management and direction of a program designed to assure the proper handling and protection of classified information, and that classified information in the Agency's possession bears the appropriate classification markings. He also will assure that the program operates in accordance with the policy established herein, and will serve as Secretary of the Classification and Declassification Committee.

(c) Assistant Administrators, Regional Administrators, Heads of Staff Offices, Directors of National Environmental Research Centers are responsible for designating an official within their respective areas who shall be responsible for:

(1) Serving as that area's liaison with the Director, Security and Inspection Division, for questions or suggestions concerning security classification matters.

(2) Reviewing and approving, as the representative of the contracting offices, the DD Form 254, Contract Security Classification Specification, issued to contractors.

(d) Employees; (1) Those employees generating documents incorporating classified information properly originated by other agencies of the Federal Government are responsible for assuring that the documents are marked in a manner consistent with security classification assignments.

(2) Those employees preparing information for public release are responsible for assuring that such information is reviewed to eliminate classified information.

(3) All employees are responsible for bringing to the attention of the Director, Security and Inspection Division, any security classification problems needing resolution.

§ 11.4 Definitions.

(a) *Classified information.* Official information which has been assigned a security classification category in the interest of the national defense or foreign relations of the United States.

(b) *Classified material.* Any document, apparatus, model, film, recording, or any other physical object from which classified information can be derived by study, analysis, observation, or use of the material involved.

(c) *Marking.* The act of physically indicating the classification assignment on classified material.

(d) *National security information.* As used in this order this term is synonymous with ''classified information.'' It is any information which must be protected against unauthorized disclosure

in the interest of the national defense or foreign relations of the United States.

(e) *Security classification assignment.* The prescription of a specific security classification for a particular area or item of information. The information involved constitutes the sole basis for determining the degree of classification assigned.

(f) *Security classification category.* The specific degree of classification (Top Secret, Secret or Confidential) assigned to classified information to indicate the degree of protection required.

(1) *Top Secret.* Top Secret refers to national security information or material which requires the highest degree of protection. The test for assigning Top Secret classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of ''exceptionally grave damage'' include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security. This classification shall be used with the utmost restraint.

(2) *Secret.* Secret refers to that national security information or material which requires a substantial degree of protection. The test for assigning Secret classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of ''serious damage'' include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; and compromise of scientific or technological developments relating to national security. The classification Secret shall be sparingly used.

(3) *Confidential.* Confidential refers to that national security information or material which requires protection. The test for assigning Confidential classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security.

§ 11.5 Procedures.

(a) *General.* Agency instructions on access, marking, safekeeping, accountability, transmission, disposition, and destruction of classification information and material will be found in the EPA Security Manual for Safeguarding Classified Material. These instructions shall conform with the National Security Council Directive of May 17, 1972, governing the classification, downgrading, declassification, and safeguarding of National Security Information.

(b) *Classification.* (1) When information or material is originated within EPA and it is believed to require classification, the person or persons responsible for its origination shall protect it in the manner prescribed for protection of classified information. The information will then be transmitted under appropriate safeguards to the Director, Security and Inspection Division, who will forward it to the department having primary interest in it with a request that a classification determination be made.

(2) A holder of information or material which incorporates classified information properly originated by other agencies of the Federal Government shall observe and respect the classification assigned by the originator.

(3) If a holder believes there is unnecessary classification, that the assigned classification is improper, or that the document is subject to declassification, he shall so advise the Director, Security and Inspection Division, who will be responsible for obtaining a resolution.

(c) *Downgrading and declassification.* Classified information and material officially transferred to the Agency during its establishment, pursuant to Reorganization Plan No. 3 of 1970, shall be declassified in accordance with procedures set forth below. Also, the same procedures will apply to the declassification of any information in the Agency's possession which originated in departments or agencies which no longer exist, except that no declassification will occur in such cases until other departments having an interest in the subject matter have been consulted. Other classified information in the Agency's possession may be downgraded or declassified by the official authorizing its classification, by a successor in capacity, or by a supervisory official of either.

(1) *General Declassification Schedule*—(i) *Top Secret.* Information or material originally classified Top Secret shall become automatically downgraded to Secret at the end of the second full calendar year following the year in which it was originated, downgraded to Confidential at the end of the fourth full calendar year following the year in which it was originated, and declassified at the end of the 10th full calendar year following the year in which it was originated.

(ii) *Secret.* Information and material originally classified Secret shall become automatically downgraded to Confidential at the end of the second full calendar year following the year in which it was originated, and declassified at the end of the eighth full calendar year following the year in which it was originated.

(iii) *Confidential.* Information and material originally classified Confidential shall become

automatically declassified at the end of the sixth full calendar year following the year in which it was originated.

(2) *Exemption from the General Declassification Schedule.* Information or material classified before June 1, 1972, assigned to Group 4 under Executive Order No. 10501, as amended, shall be subject to the General Declassification Schedule. All other information or material classified before June 1, 1972, whether or not assigned to Groups 1, 2, or 3, of Executive Order No. 10501, as amended, shall be excluded from the General Declassification Schedule. However, at any time after the expiration of 10 years after the date of origin it shall be subject to a mandatory classification review and disposition in accordance with the following criteria and conditions:

(i) It shall be declassified unless it falls within one of the following criteria:

(*a*) Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence.

(*b*) Classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods.

(*c*) Classified information or material disclosing a system, plan, installation, project, or specific foreign relations matter, the continuing protection of which is essential to the national security.

(*d*) Classified information or material the disclosure of which would place a person in immediate jeopardy.

(ii) *Mandatory review of exempted material.* All classified information and material originated after June 1, 1972, which is exempted under any of the above criteria shall be subject to a classification review by the originating department at any time after the expiration of 10 years from the date of origin provided:

(*a*) A department or member of the public requests a review;

(*b*) The request describes the document or record with sufficient particularity to enable the department to identify it; and

(*c*) The record can be obtained with a reasonable amount of effort.

(*d*) Information or material which no longer qualifies for exemption under any of the above criteria shall be declassified. Information or material which continues to qualify under any of the above criteria shall be so marked, and, unless impossible, a date for automatic declassification shall be set.

(iii) All requests for ''mandatory review'' shall be directed to:

Director, Security and Inspection Division, Environmental Protection Agency, Washington, DC 20460.

The Director, Security and Inspection Division shall promptly notify the action office of the request, and the action office shall immediately acknowledge receipt of the request in writing.

(iv) *Burden of proof for administrative determinations.* The burden of proof is on the originating Agency to show that continued classification is warranted within the terms of this paragraph (c)(2).

(v) *Availability of declassified material.* Upon a determination under paragraph (ii) of this paragraph (c)(2), that the requested material no longer warrants classification, it shall be declassified and made promptly available to the requester, if not otherwise exempt from disclosure under section 552(b) of Title 5 U.S.C. (Freedom of Information Act) or other provision of law.

(vi) *Classification review requests.* As required by paragraph (ii) of this paragraph (c)(2) of this order, a request for classification review must describe the document with sufficient particularity to enable the Department or Agency to identify it and obtain it with a reasonable amount of effort. Whenever a request is deficient in its description of the record sought, the requester should be asked to provide additional identifying information whenever possible. Before denying a request on the ground that it is unduly burdensome, the requester should be asked to limit his request to records that are reasonably obtainable. If nonetheless the requester does not describe the records sought with sufficient particularity, or the record requested cannot be obtained with a reasonable amount of effort, the requester shall be notified of the reasons why no action will be taken and of his right to appeal such decision.

§ 11.6 Access by historical researchers and former Government officials.

(a) Access to classified information or material may be granted to historical researchers or to persons who formerly occupied policymaking positions to which they were appointed by the President: *Provided, however,* That in each case the head of the originating Department shall:

(1) Determine that access is clearly consistent with the interests of the national security; and

(2) Take appropriate steps to assure that classified information or material is not published or otherwise compromised.

(b) Access granted a person by reason of his having previously occupied a policymaking position shall be limited to those papers which the former official originated, reviewed, signed, or received while in public office, except as related to the ''Declassification of Presidential Papers,'' which shall be treated as follows:

(1) *Declassification of Presidential Papers.* The Archivist of the United States shall have authority

to review and declassify information and material which has been classified by a President, his White House Staff or special committee or commission appointed by him and which the Archivist has in his custody at any archival depository, including a Presidential library. Such declassification shall only be undertaken in accord with:

(i) The terms of the donor's deed of gift;

(ii) Consultations with the Departments having a primary subject-matter interest; and

(iii) The provisions of § 11.5(c).